LEARNING LESSONS FROM CLOUD INVESTIGATIONS IN EUROPE: BARGAINING ENFORCEMENT AND MULTIPLE CENTERS OF REGULATION IN DATA PROTECTION

Asma A.I. Vranaki†

Abstract

The race is on for businesses and consumers to join the cloud. From increased efficiency to low operational costs to scalability, reasons abound as to why we are adopting cloud solutions. However, unleashing the potential of cloud ecosystems for companies and individuals has not been without difficulties. Industry research has highlighted that data protection and privacy concerns, in particular, can often be one of the main inhibitors to the widespread adoption of cloud-based systems. Lately, some U.S.-based cloud companies have been required to comply with European data protection laws through the regulatory process of investigation by European data protection authorities ("Cloud Investigations").

In this Article, I analyze selected empirical findings from my recent qualitative socio-legal research project where I have examined the investigations of companies providing cloud-based services ("Cloud Providers") by European data protection authorities (EU DPAs) to reflect on the roles of data protection laws during such investigations.

I advance two arguments. First, a decentralized perspective on Cloud Investigations sheds a more comprehensive light on the roles of data protection laws during Cloud Investigations without assuming a priori *that such laws have a privileged and static role in the regulatory process.*

Second, and relatedly, I argue that by "cutting off the King's head," we can understand more fully the dynamic and context-dependent roles of data protection laws during Cloud Investigations. From time to time, law can be deployed to achieve the aims of the lawmakers or enforcers. At other times, law can also be used as bargaining chips by EU DPAs and Cloud Providers to

† This Article is derived from the research that the author has undertaken for the "Accountability for Cloud" research project, which was funded by the European Commission Seventh Framework Programme. All references in this Article were current as at the time of writing.

obstruct or facilitate the negotiations during Cloud Investigations. At other times still, law can often retreat from the field of action as other actors carry out the "act of government" to determine if and to what extent Cloud Providers are "accountable in reality."

TABLE OF CONTENTS

I. INTRODUCTION

The race is on for businesses and consumers to join the cloud. From increased efficiency to low operational costs to scalability, reasons abound for why we are adopting cloud solutions. Beyond the buzzwords, what is the cloud? There is no single agreed-upon definition of cloud computing. In essence, this term refers to the delivery of computing resources (for example, storage) as a service through a network (such as the Internet) on a scalable, pay-by-use (if not free) and on-demand basis.[1]

Industry research has highlighted that regulatory and legal issues, such as data protection and privacy issues, can prevent the widespread adoption of cloud-based systems.[2] For example, a cloud solution can involve a complex chain of Cloud Providers.[3] In data protection terms, this may lead to several problems, including difficulties in determining which Cloud Providers are acting as data "controllers" or data "processors."[4] The data

1. INFO. COMM'R'S OFFICE, GUIDANCE ON THE USE OF CLOUD COMPUTING 3–4 (Feb. 10, 2012), https://ico.org.uk/media/1540/cloud_computing_guidance_for_organisations.pdf.

2. *See Industry's Largest Cloud Computing Survey Reveals 5x Adoption of SaaS*, NORTH BRIDGE, http://www.northbridge.com/industry-largest-cloud-computing-survey-reveals-5x-adoption-saas (last visited Sept. 13, 2016) (noting data security concerns serve as cloud inhibitors).

3. INFO. COMM'R'S OFFICE, *supra* note 1, at 4, 6.

4. *See* W. Kuan Hon et al., *What Is Regulated as Personal Data in Clouds?*, *in* CLOUD COMPUTING LAW 167, 168–83 (Christopher Millard ed., 2013) (explaining the difficulties in identifiability of controllers or processors). A European Parliament directive defines "controller" as a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data." Directive 95/46/EC, art. 2(d), of the European Parliament and of the Council

"controller"/"processor" categorization is crucial under the current European data protection laws to determine and allocate data protection responsibilities.

Lately, European data protection authorities (EU DPAs) have investigated many U.S.-based cloud companies ("Cloud Investigations").[5] That European regulators have so far investigated mostly U.S.-based cloud companies is perhaps not surprising, given that such companies have a sizeable market share of the European cloud market.[6] EU DPAs are the statutory independent public regulatory bodies that have many functions, including enforcing data protection laws in the European Economic Area (EEA).[7] Investigations refer to the power of EU DPAs to investigate data "controllers," such as companies providing cloud-based services ("Cloud Providers"), in specific circumstances, including when an individual complains.[8] The increase in Cloud Investigations raises interesting questions about how "personal data" are regulated by the regulatory tool of investigation and the roles of data protection laws during Cloud Investigations. "Personal data" means "any information relating to an identified or identifiable natural person."[9]

Current data protection literature adopts a state-centric approach to data protection laws.[10] From this viewpoint, data protection laws are viewed as static regulatory tools that are deployed in only one direction (for example, from the EU DPA to the Cloud Provider) to achieve the aims of the state through its legislative draftspersons and enforcers.[11] As an illustration, many scholars approach data protection laws solely as binding rules—imposed by

---

of 24 October 1995, 1995 O.J (L 281) 31, 38 [hereinafter Data Protection Directive], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046. The Data Protection Directive defines "processor" as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." *Id.* art. 2(e). The Data Protection Directive will be replaced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR], http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. The GDPR enters into force on May 24, 2016 and will apply on May 25, 2018. *Id.* art. 99.

5. *See, e.g.*, Press Release, Commission Nationale de l'Informatique et des Libertés (CNIL), Google's New Privacy Policy: Incomplete Information and Uncontrolled Combination of Data Across Services (Oct. 16, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_press_release_google_privacy_cnil_en.pdf (providing details of such Cloud Investigations).

6. Other factors, such as media reports of data breaches by U.S.-based Cloud Providers and complaints filed by EU-resident users, can also account for why U.S.-based Cloud Providers have been investigated. *See* Interview 1, *infra* note 140. The interviews on which this Article is based are set forth in notes 140–42, *infra*.

7. Data Protection Directive, *supra* note 4, art. 28. In different jurisdictions, several labels are used to denote the statutory independent public regulatory body that has the function of applying and enforcing data protection laws. For example, in the UK the DPA is referred to as the "Information Commissioner" whereas in Italy the DPA is referred to as "Il Garante per la protezione dei dati personali." Some legislative frameworks, such as the Data Protection Directive, *supra* note 4, use the term "supervisory authorities" to refer to such bodies.

8. *Id.* art. 28(3).

9. *Id.* art. 2(a).

10. *E.g.*, András Jóri, *Shaping vs Applying Data Protection Law: Two Core Functions of Data Protection Authorities*, 5 INT'L DATA PRIVACY L. 133 (2015); Maria Stella Righettini, *Institutionalization, Leadership, and Regulative Policy Style: A France/Italy Comparison of Data Protection Authorities*, 13 J. COMP. POL'Y ANALYSIS 143 (2011).

11. *Id.*

the state from a top-down direction—that create new legal obligations, powers, and actors, such as EU DPAs.[12] Such scholars tend to analyze data protection laws from a mostly textual perspective.[13] For instance, some writers focus on analyzing the inconsistent implementation of the Data Protection Directive.[14] The Data Protection Directive regulates the processing of personal data in EEA countries.[15]

Data protection laws often seem to have a privileged role in regulating "personal data" in such writings because they are approached as the sole or principal objects of analysis.[16] More recent works on data protection laws concede that social interactions, such as discussions among regulators, can also have an impact on how data protection laws are applied in practice.[17] However, such works still approach investigations as tools that are deployed in one direction, namely from the regulator to the regulatee, to achieve only the aims of the state as envisaged by the lawmakers and law enforcers.[18]

In this Article, I analyze selected empirical findings from my recent qualitative socio-legal research project[19] where I have examined EU DPAs' investigations of Cloud Providers to reflect on the roles of data protection laws during Cloud Investigations. I understand data protection laws as encompassing the relevant European directives and regulation, national data protection and related procedural laws, rulings from the national and European courts, and the guidance or the opinions from EU DPAs and the Article 29 Working Party (A29WP).[20] Consequently, my understanding of law also encompasses "soft" laws, including the non-binding A29WP opinions.

I advance two arguments. First, a decentralized perspective on Cloud Investigations sheds a more comprehensive light on the roles of data protection laws during those investigations without assuming *a priori* that such laws have a privileged and static role in the regulatory process. Second, I argue that by "cutting off the King's head," we can understand more fully the dynamic and context-dependent roles of data protection laws during Cloud Investigations. From time to time, law can be deployed to achieve the aims of the lawmakers

12. Data Protection Directive, *supra* note 4, art. 28.

13. *Id.*

14. *E.g.*, LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS (2002) (analyzing data protection laws); Jóri, *supra* note 10.

15. Data Protection Directive, *supra* note 4, art. 1(1).

16. *See, e.g.*, Charles D. Raab, *Networks for Regulation: Privacy Commissioners in a Changing World*, 13 J. COMP. POL'Y ANALYSIS 195 (2011) (analyzing the influential relationship between data protection laws and personal data).

17. *See, e.g.*, *id.*

18. *See, e.g.*, *id.*

19. "Socio-legal studies" refers to the study of law in context. *See generally* DENIS J. GALLIGAN, LAW IN MODERN SOCIETY (2007).

20. Relevant European directives include the Data Protection Directive, *supra* note 4, and Directive 2002/58/EC, 2002 O.J. (L 201) 37. The A29WP is an advisory body that is composed of representatives of the EU DPAs, the European Data Protection Supervisor, and the European Commission. *Article 29 Working Party*, EUR. COMM'N, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm (last updated June 10, 2015). Relevant A29WP opinions include Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor," 264/10/EN, WP 169 (Feb. 16, 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

or enforcers. At other times, law can also be used as bargaining chips by EU DPAs and Cloud Providers to obstruct or facilitate the negotiations during Cloud Investigations. At other times still, law can retreat from the field of action as other actors regulate "personal data" to determine if and to what extent Cloud Providers are "accountable in reality."[21]

I pursue these arguments in the remaining six Parts. Part II of this Article begins by providing a brief introduction to cloud computing and the data protection issues that can be raised by such technologies. Part III goes on to critically evaluate some of the main provisions of the European data protection laws that apply to Cloud Investigations. Part IV conceptualizes law in broader terms than a mere norm issued by the sovereign state, which is backed by sanctions and enforced by specific actors. Part V explains the methodology of this Article. In Part VI, I analyze selected empirical findings to evaluate how EU DPAs and Cloud Providers can often strategically use data protection laws in ways that have not been anticipated by the legislative draftsperson or enforcer, namely as bargaining tools. Finally, in Part VII, I consider how multiple "centers of calculation" (for example, technological, social, and legal) rather than merely legal "centers of calculation" are involved during Cloud Investigations to highlight that data protection laws do not have a privileged and static role during Cloud Investigations.

II. A PRIMER ON CLOUD COMPUTING

The rapid pace of innovation in the information and communications technology sector means that we often encounter a new term like "cloud computing" that encapsulates an emerging innovation with a number of technical and commercial characteristics. In this Part, I introduce the reader to cloud computing by paying attention to its service and deployment models. I also underline how the data protection concerns raised by cloud ecosystems are very much tied to how such ecosystems are configured in terms of their service and deployment layers.

For many, cloud computing signals a new phase in computing as it enables its users to access computing resources, such as storage and processing, stored on shared and remote systems, on-demand, irrespective of location, on an agile basis with metered pricing (if any) through a network.[22] Through its characteristics, including pooling, scalability, and on-demand, cloud computing enables its users to reduce their capital expenditure (such as the costs of purchasing hardware) and incur only operational costs.[23] As an example, the website of a fashion store can often receive a high level of traffic at variable times, such as during the bank holiday sales. Consequently, the store needs the flexibility to double or triple how much traffic its website can

21. Interview 1, *infra* note 140.

22. *Easiest Way to Understand Cloud Computing*, BISINFOTECH (Aug. 8, 2015), http://www.bisinfotech.com/blog/what-is-cloud-computing/.

23. *Id.*

handle during these peak times. If the store hosts its website on a cloud server, such as Storm on Demand, with a few clicks the store can instantaneously provision its server so that its website can handle the increased traffic level and scale it back down again after the traffic levels return to normal.[24] The fashion store is billed on a metered basis, which means that it pays for only the utilized resources.[25] This can be a far more cost-effective solution for the store than using a dedicated hosting solution, which would require the store to invest in, configure, and maintain a more powerful machine as well as retain the machine even when traffic levels have decreased.[26]

Cloud services can be characterized by their service and deployment models. In terms of service models, cloud-based solutions can involve one or more service models, typically Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[27] Put simply, an IaaS cloud (for example, Amazon's Elastic Compute Cloud) offers access to raw computing resources, such as computing hardware.[28] A PaaS cloud, such as Google App Engine, offers access to a computing platform that enables its customers to develop and run software applications.[29] An SaaS cloud (Dropbox is an example of an SaaS cloud) offers its users access to a complete software application through a network.[30] Cloud solutions can often involve different layers of cloud services, which results in a complex supply chain that may not always be apparent to the end user.[31] As an illustration, a company can offer a calendar software to its clients as an SaaS. However, the company hosts the software on an IaaS cloud that is owned and operated by another company. In this example, it is often difficult for the end users to know which providers or sub-providers, other than the SaaS provider, are involved in delivering this service and the data protection responsibilities of such sub-providers and providers.

Cloud-based solutions can be delivered in various ways. Typically, there are four main deployment models: private cloud, community cloud, public cloud, and hybrid cloud.[32] In plain terms, a private cloud provides computing resources as a service within a virtualized environment using an underlying

24. *Cloud Hosting—A New Way to Think*, STORM ON DEMAND, http://www.stormondemand.com/servers/ (last visited Sept. 13, 2016).

25. *Pricing*, STORM ON DEMAND, http://www.stormondemand.com/pricing (last visited Sept. 13, 2016).

26. SIANI PEARSON, HP LABS, UK, PRIVACY, SECURITY AND TRUST IN CLOUD COMPUTING 2 (June 28, 2012), http://www.hpl.hp.com/techreports/2012/HPL-2012-80R1.pdf; *Types of Hosting Services: From Shared Hosting to Cloud Servers (Infographic)*, ELASTICHOSTS (Apr. 12, 2016), https://www.elastichosts.com/blog/from-shared-hosting-to-cloud-vps/.

27. *Demystifying SaaS, PaaS, and IaaS*, SKYTAP (Mar. 22, 2011), https://www.skytap.com/blog/demystifying-saas-paas-and-iaas/.

28. *Amazon EC2—Virtual Server Hosting*, AMAZON WEB SERVS., https://aws.amazon.com/ec2/ (last visited Sept. 13, 2016).

29. *App Engine*, GOOGLE CLOUD PLATFORM, https://cloud.google.com/appengine/ (last visited Sept. 13, 2016).

30. DROPBOX, https://www.dropbox.com/ (last visited Sept. 13, 2016).

31. Article 29 Data Protection Working Party, Opinion 5/2012 on Cloud Computing, 1037/12/EN, WP 196, at 6 (July 1, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

32. *Id.* at 25.

pool of computing resources.[33] The client benefits from the advantages of cloud computing, such as self-service and agility, while having greater control over the cloud environment because the client is the only entity that can access the pool of resources.[34] Community clouds refer to cloud environments that are shared among limited groups of users with common requirements, such as security and privacy.[35] Public clouds refer to cloud environments that are shared among multiple users who utilize the same computing resources, such as servers and storage.[36] Finally, hybrid clouds involve a mix of private, community, and public clouds.[37] One of the main differences between these four deployment models is that they provide their users with varying levels of control over data, which can lead to data protection issues. For example, there are concerns about unauthorized data access in multi-tenant public cloud environments.[38] In some cases, unauthorized data access can be addressed by various measures, including devising robust access policies and partitioning the data of tenants.[39] However, in other cases, such as when sensitive personal data (for example, financial data) are processed in a public cloud, such measures may still be insufficient to ensure regulatory compliance.[40]

III. CLOUD INVESTIGATIONS AND DATA PROTECTION LAWS: A CRITICAL EVALUATION

Having explained some of the main characteristics of cloud computing and that the data protection concerns raised by cloud ecosystems are tied to these characteristics, in this Part, I critically analyze some of the main provisions of the Data Protection Directive that apply to Cloud Investigations. The Data Protection Directive provides the point of departure for most of the analysis, because EU DPAs apply the directive as nationally implemented.[41] Where relevant, I also discuss the national implementing laws.

The Data Protection Directive has several aims, including harmonizing European data protection laws, protecting the fundamental rights and freedoms of individuals, and promoting the trans-border flow of personal data.[42] To

33. *Id.*
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.*
38. Press Release, Gartner, Gartner Says 60 Percent of Virtualized Servers Will Be Less Secure than the Physical Servers They Replace Through 2012 (Mar. 15, 2010), http://www.gartner.com/newsroom/id/1322414.
39. *Id.*
40. THOMAS HAEBERLEN & LIONEL DUPRÉ, EUR. NETWORK & INFO. SEC. AGENCY, CLOUD COMPUTING: BENEFITS, RISKS AND RECOMMENDATIONS FOR INFORMATION SECURITY 22 (Dec. 2012), https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security.
41. Data Protection Directive, *supra* note 4, art. 2; EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS, DATA PROTECTION IN THE EUROPEAN UNION: THE ROLE OF NATIONAL DATA PROTECTION AUTHORITIES 19 (Nov. 28, 2010) [hereinafter ROLE OF DPAS], http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf.
42. Data Protection Directive, *supra* note 4, art. 2. Such aims did not exist in a state of nature but

achieve these aims, the Data Protection Directive has established new legal actors (such as EU DPAs), rights, and obligations.[43] The Data Protection Directive endows EU DPAs with a number of powers, including intervention and investigation.[44] EEA countries have a large degree of discretion when they implement the Data Protection Directive nationally because many provisions of the Directive—including Article 28, the main provision setting out the investigatory powers of EU DPAs—are very broad and vague.[45] Depending on the aims and foci of the investigations, other provisions of the Data Protection Directive may also be relevant.

My empirical analysis has highlighted that, at a baseline, most Cloud Investigations aim to assess the legal compliance of Cloud Providers and enforce data protection laws in cases of non-compliance.[46] However, depending on the context, some Cloud Investigations can also have other aims, including encouraging the Cloud Provider to adopt "best practice" recommendations that go beyond the letter of the law and educating the Cloud Provider about its data protection obligations.[47] Cloud Investigations can also have different foci. Some Cloud Investigations can focus on a limited number of processing operations and policies while other investigations can evaluate all the operations and policies of the company.[48]

Four key issues are raised when the sweeping and indeterminate provisions of the Data Protection Directive—as nationally implemented—are applied to Cloud Investigations.

First, Article 28(1) of the Data Protection Directive provides that EU DPAs should be fully autonomous regulatory bodies.[49] In essence, this means that EU DPAs should not allow their administrative dependence on other actors, such as their financial dependence on governmental departments, to have an impact on their functional independence.[50] Despite the salience of the independence criterion in the European data protection law regime, a recent review of the implementation of the Data Protection Directive by the EEA countries has highlighted that many EU DPAs have still not achieved full independence from other actors due to their limited financial resources.[51] This

emanated from their interactions with other relevant actors, such as national Member States and European institutions.

43. *See*, *e.g.*, *id.* art. 12 (providing "data subjects" with access rights); *id.* art. 2(h) (defining a "data subject" as an "identified or identifiable natural person").

44. *Id.* art. 28(3).

45. *Id.* art. 28.

46. *E.g.*, Interviews 1 & 2, *infra* note 140.

47. *Id.*

48. *E.g.*, Interviews 1, 2 & 3, *infra* note 140.

49. Data Protection Directive, *supra* note 4, art. 28(1).

50. *Id.* The Court of Justice of the European Union has ruled that the "decision-making power [of EU DPAs should be] independent of any direct or indirect external influence." Case C-518/07, Comm'n v. Germany, 2010 E.C.R. I-1885, ¶ 19 (2010), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62007CJ0518.

51. *See Commission First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 12–13, COM (2003) 265 final (May 15, 2003) [hereinafter *Commission First Report*], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF (reviewing member state implementation of the Data Protection Directive); ROLE OF DPAS, *supra* note 41 (analyzing data protection

can potentially raise issues about how and to what ends some EU DPAs exercise their powers, including their investigative powers. In particular, my findings on how some EU DPAs manage their limited resources by using the assistance of other actors (for example, sub-contractors financed by the investigated Cloud Providers) raise critical questions about the potential influence of such actors during Cloud Investigations.[52] To what extent might the Cloud Provider be able to influence the technical testing stage of the Cloud Investigation when it fully or partially bears the costs of hiring an independent technical expert? EU DPAs can put in place safeguards, including contractual clauses, providing that the expert will act only under the strict instructions of the regulator.[53] However, even in such cases, it is possible that such financial arrangements may affect the outcomes of the investigation.[54]

Second, although Article 28 of the Data Protection Directive endows EU DPAs with many powers, including investigative and intervention powers, the inconsistent implementation of the directive means that many EU DPAs are still not endowed with full powers.[55] As an example, the Hellenic DPA does not have the power to bring a case directly before the judicial authorities.[56] This may have an impact on the range of actions available to EU DPAs if a Cloud Provider refuses to implement some of its recommendations after a Cloud Investigation.[57] Even in cases in which EU DPAs have similar powers, such as the powers to impose a monetary penalty, there can still be national differences.[58] EU DPAs can often have different maximum fine levels.[59] In practice, this means that there can often be inconsistent sanctions applied by EU DPAs after Cloud Investigations. When EU DPAs impose varying sanctions when investigating the same Cloud Provider for substantially similar breaches, this can have an impact on the effectiveness of the law's sanctioning powers.[60]

Recently, some EU DPAs have imposed different levels of fines following their investigations into the compliance of the privacy policy of

---

authorities and their effectiveness in protecting fundamental rights in data protection).

52. *E.g.*, Interviews 1 & 4, *infra* note 140.

53. Asma Vranaki, *Cloud Investigations by European Data Protection Authorities: An Empirical Account*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 518 (John Rothchild ed., 2016).

54. *Id.*

55. *See Commission First Report*, *supra* note 51, at 13.

56. Nomos (1997:2472) Prostasia toy Atomoy apo thn Epexergasia Dedomenwn Proswpikoy Charakthra [on the Protection of Individuals with Regard to the Processing of Personal Data], EPHEMERIS TES KYVERNESEOS TES HELLENIKES DEMOKRATIAS [E.K.E.D.] 1997, B:967, art. 19(1)(e) (Greece), http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%202472-97-NOV2013-EN.PDF.

57. Vranaki, *supra* note 53.

58. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, ACCESS TO DATA PROTECTION REMEDIES IN EU MEMBER STATES 21 (2013) [hereinafter DATA PROTECTION REMEDIES], http://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf.

59. *Id.*

60. Recent research by the European Agency for Fundamental Rights concludes that the inconsistent fining powers of EEA countries is an obstacle to the effectiveness of the Data Protection Directive. *See* DATA PROTECTION REMEDIES, *supra* note 58.

Google Inc. ("Google") with the applicable data protection laws.[61] For example, the French DPA levied a maximum fine of €150,000 against Google and also required the company to display its order on the company's website for forty-eight hours.[62] The Spanish DPA fined Google €900,000, while the Dutch DPA will impose an incremental penalty payment amounting to €15 million if Google fails to implement specific changes by a set deadline.[63] On the other side of the English Channel, the UK DPA recently opted not to fine Google and successfully negotiated an undertaking that requires Google to implement specific changes to its privacy policy within a prescribed time frame.[64] Many stakeholders have criticized the divergent approaches of the EU DPAs in the Google investigations.[65]

Third, Article 28(3) of the Data Protection Directive specifies some of the investigative powers of an EU DPA: "powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties."[66] As this provision does not provide an exhaustive list of the investigative tasks of EU DPAs, these tasks have been inconsistently fleshed out either in national implementing laws or through the practices of EU DPAs.[67] As an illustration, EU DPAs, such as the French DPA, have the power to undertake online inspections, while others do not.[68] It also means that non-legal factors, such as financial or external pressures faced by EU DPAs, can often have an impact on the tasks deployed during an investigation.[69] For instance, some of the smaller

61. *See, e.g.*, Commission Nationale de l'Informatique et des Libertés [CNIL] [National Commission for Information Technology and Civil Liberties], June 10, 2013, Decision No. 2013-025 Giving Formal Notice to the Company Google Inc. [hereinafter CNIL Decision], http://www.cnil.fr/fileadmin/documents/en/D2013-025_10_Jun_2013_GOOGLE_INC_EN.pdf (ordering Google to comply with the French Data Protection Act).

62. *See* Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, art. 45, § I, *amended by* Law 2004-801 of Aug. 6, 2004, http://www.legislationline.org/download/action/download/id/1245/file/2c6afeb365cf84afa6d0de952262.pdf (listing sanctions that the Commission may impose); *Google Served Maximum Fine by French Data Protection Authority over Privacy Policy Failings*, OUT-LAW.COM (Jan. 10, 2014), http://www.out-law.com/en/articles/2014/january/google-served-maximum-fine-by-french-data-protection-authority-over-privacy-policy-failings/.

63. Press Release, Dutch Data Prot. Auth., CBP Issues Sanction to Google for Infringements Privacy Policy (Dec. 15, 2014), https://cbpweb.nl/en/news/cbp-issues-sanction-google-infringements-privacy-policy.

64. Data Protection Act 1998 (UK) Undertaking, by Kent Walker, Senior Vice-President & General Counsel of Google Inc., on behalf of Google Inc. (Jan. 30, 2015), https://ico.org.uk/media/action-weve-taken/undertakings/1043170/google-inc-privacy-policy-undertaking.pdf. For more on the UK DPA's power to impose a monetary penalty, see Data Protection Act 1998 (UK), §§ 55A–E (UK).

65. *See, e.g.*, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, at 5, COM (2013) 847 final (Nov. 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

66. Data Protection Directive, *supra* note 4, art. 28(3).

67. J. C. Bruno & Elsa Crozatier, *Compliance with the European Union Directive in the Transfer of Employee Personal Data to U.S. Affiliates*, MICH. B.J., Nov. 2004, at 48.

68. Loi 2014-344 du 17 mars 2014 relative à la consommation, [Law 2014-344 of March 17, 2014 on Consumption], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028738036&categorieLien=id.

69. *See, e.g.*, Interviews 1, 2 & 3, *infra* note 140.

EU DPAs with limited financial resources tend to favor investigative practices that are not as draining on their resources. Contract and code review are examples of these types of tasks.[70] This divergence can often have an impact on the outcomes of investigations generally. In the cloud context, depending on the Cloud Investigation in question, EU DPAs that carry broader and more detailed investigative tasks (such as code testing rather than code review) are more likely to generate a fuller evaluation of the Cloud Provider's legal compliance than the regulators who do not conduct such detailed compliance assessments.[71]

Fourth, the wide ambit of Article 28 also means that certain aspects of Cloud Investigations, such as what the Cloud Provider can expect before, during, and after a Cloud Investigation, are inconsistently fleshed out at a national level.[72] Consequently, investigated Cloud Providers can often encounter varying degrees of openness, transparency, and consistency in different jurisdictions.[73] It is evident that European laws have to be transposed in such a way that they are compatible with the legal system of each EEA country.[74] However, the inconsistent guidance that EU DPAs provide to Cloud Providers on Cloud Investigations causes significant problems for such companies.[75] Such organizations have more or less information about the process in question depending on the territory in question.[76] For example, while jurisdictions like Ireland are relatively open and transparent about how they conduct their investigations, other jurisdictions, such as France, do not have similar public guidance.[77]

---

70. Interview 3, *infra* note 140.

71. *Id.*

72. *Compare* Data Protection Act 1988 (Act No. 25/1988) (Ir.), § 24, *amended by* Data Protection (Amendment) Act 2003 (Act. No. 6/2003) (Ir.) (giving the Irish DPA the power to authorize a person, including another EU DPA, in writing, to exercise a number of powers during investigations, including the power to obtain information from the investigated data controller) *with* Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, *amended by* Law 2004-801 of Aug. 6, 2004 *and* Décret 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertésthe [Decree 2005-1309 of October 20, 2005 enacted for the application of Act No 78-17 of January 6, 1978 on Data Processing, Files and Individual Liberties], *amended by* Decree 2007-451 of March 25, 2007 (regulating the investigative powers of the French DPA but not authorizing the French DPA to appoint another party as an "authorised officer" during its investigations); *see also* Caroline Donnelly, *EU Data Protection Regulation: What the EC Legislation Means for Cloud Provider*s, COMPUTER WEEKLY (Oct. 9, 2015), http://www.computerweekly.com/feature/EU-Data-Protection-Regulation-What-the-EC-legislation-means-for-cloud-providers.

73. *See, e.g.*, Cloud Provider Interviews, *infra* note 141.

74. Consolidated Version of the Treaty on the Functioning of the European Union, 2008 O.J. C 115/47.

75. *See, e.g.*, Article 29 Data Protection Working Party, Declaration of the Article 29 Working Party on Enforcement, 12067/04/EN, WP 101 (Nov. 25, 2004), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp101_en.pdf (making the case for the need to overcome national differences and move towards "synchronized national enforcement actions"); Yves Poullet, *EU Data Protection Policy. The Directive 95/46/EC: Ten Years After*, 22 COMPUTER L. & SEC. R. 206, 207 (2006) (describing the problems companies face in dealing with the "complexity of managing compliance across multiple sets of standards").

76. *See, e.g.*, Cloud Provider Interviews, *infra* note 141.

77. *See, e.g.*, OFFICE OF THE DATA PROTECTION COMM'R [OF IRELAND], GUIDE TO AUDIT PROCESS

Relatedly, many companies rely on the non-binding advice provided by EU DPAs to assess their data compliance before the start of the Cloud Investigations.[78] However, such advice can often be inconsistent with one another. As an example, the Irish DPA advises data "controllers" operating in a single tenant cloud arrangement to discharge their security obligations by directly auditing the security measures put in place by the company that provides them with their cloud-based service.[79] It is questionable to what extent it is practical and feasible for data "controllers" to directly inspect the premises of such organizations. Conversely, the UK DPA advises data "controllers" to discharge their security obligations by requiring an independent third party to conduct a detailed security audit of the cloud services they use as well as provide a copy of this assessment to their prospective customers.[80] The inconsistent advice that Cloud Providers can often receive from EU DPAs about data protection in the cloud can be partly explained by the fact that EU DPAs operate at a national rather than transnational level when producing such guidance.[81]

In practice, such inconsistent guidance means that the data "controllers" operating in various EEA countries may often have to rely on disparate national guidance when determining their data protection compliance before or during a Cloud Investigation.[82] Additionally, many of my EU DPA respondents have argued that national guidance on cloud computing plays an important role during Cloud Investigations.[83] For instance, this information guides the investigative staff of the EU DPA by reminding the team of cloud-centric matters, such as the importance of avoiding a "one size fits all"[84] approach.[85] Thus, it is crucial for such guidance to share a common baseline that reflects a European perspective on the regulation of cloud data. This is particularly important given that some Cloud Investigations can often involve formal or informal cooperation between EU DPAs.[86]

Finally, one of my key empirical findings was that so far many Cloud Investigations seem to tackle general data protection issues rather than cloud-specific ones.[87] When I raised this issue with my EU DPA respondents, they all unanimously stated that they did not view an investigation of a cloud-based

(Aug. 2014), https://www.dataprotection.ie/docimages/documents/GuidetoAuditProcessAug2014.pdf (setting out the guidance for investigations that the Irish DPA undertakes of its own volition pursuant to the Data Protection (Amendment) Act 2003, *infra* note 133, § 10(1A)).

78. *See, e.g.*, Interview 2, *infra* note 140.

79. *Data Protection "In the Cloud"*, DATA PROTECTION COMM'R [OF IRELAND] (July 3, 2012), http://www.dataprotection.ie/docs/03-07-12-Cloud-Computing/1221.htm.

80. INFO. COMM'R'S OFFICE, *supra* note 1, ¶ 58.

81. *The Proposed General Data Protection Regulation: The Consistency Mechanism Explained*, EUR. COMM'N (June 2, 2013), http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm.

82. *See, e.g.*, Cloud Provider Interviews, *infra* note 141.

83. *See id.*

84. INFO. COMM'R'S OFFICE, *supra* note 1, ¶ 35.

85. *E.g.*, Interviews 1, 2 & 3, *infra* note 140.

86. *Id.*; *see also* Vranaki, *supra* note 53.

87. *E.g.*, All Interviews, *infra* notes 140–42.

company differently from an investigation of a non-cloud-based organization.[88] This is quite surprising given the characteristics of the cloud, such as its service and deployment models, which can often give rise to specific and intricate data protection concerns.[89] Many EU DPAs publicly recognize this point.[90] As few EU DPAs have published a public report after their Cloud Investigations, it is difficult to assess precisely to what extent such investigations do or do not reflect cloud-centric issues.[91] However, my analysis of the published Cloud Investigations reports has been quite instructive on this point. Due to space constraints, I focus only on the report published by the Dutch DPA after its investigation of WhatsApp Inc. ("WhatsApp").[92] I have chosen this report because it is fairly representative of how other EU DPAs have approached cloud-centric data protection issues in their external investigation reports.

In brief, the Dutch and Canadian DPAs investigated WhatsApp in 2012 ("WhatsApp Investigation").[93] WhatsApp is a popular cross-platform[94] mobile messaging application that enables its users to send and receive different types of instant messages, including voice[95] and media[96] messages.[97] Both DPAs found WhatsApp in breach of their national data protection laws for several

88. *E.g.*, Interviews 1, 2, 3 & 4, *infra* note 140.

89. Jaydip Sen, *Security and Privacy Issues in Cloud Computing*, *in* STANDARDS AND STANDARDIZATION: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS 1376–78 (2015).

90. *See, e.g.*, *Data Protection "In the Cloud"*, *supra* note 79; INFO. COMM'R'S OFFICE, *supra* note 1.

91. *See, e.g.*, Article 29 Data Protection Working Party, Google Privacy Policy: Main Findings and Recommendations, Oct. 16, 2012, app. to Article 29 Letter, *infra* note 137 [hereinafter Article 29 Main Findings], http://www.cnil.fr/fileadmin/documents/en/GOOGLE_PRIVACY_POLICY-_RECOMMENDATIONS-FINAL-EN.pdf; DATA PROTECTION COMM'R [OF IRELAND], FACEBOOK IRELAND LTD: REPORT OF AUDIT (Dec. 21, 2011), http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf; CNIL Decision, *supra* note 61, at 6. The CNIL decision is not a "report" as such but rather a formal notice issued by the French DPA to Google Inc. following its investigation of the compliance of the privacy policies of Google Inc. with French data protection laws. CNIL Decision, *supra* note 61. However, this formal decision highlights the main axes of evaluation and decision-making carried out during the investigation. *Id.*

92. *See* DUTCH DATA PROT. AUTH., REPORT ON THE DEFINITIVE FINDINGS OF THE INVESTIGATION INTO THE PROCESSING OF PERSONAL DATA FOR THE "WHATSAPP" MOBILE APPLICATION BY WHATSAPP INC. (informal trans., Jan. 15, 2013) [hereinafter WHATSAPP FINDINGS], https://cbpweb.nl/sites/default/files/downloads/mijn_privacy/rap_2013-whatsapp-dutchdpa-final-findings-en.pdf.

93. *Id.*

94. *See About WhatsApp*, WHATSAPP, https://www.whatsapp.com/about/ (last visited Sept. 13, 2016). WhatsApp can be used on various mobile operating systems including Android, Windows Phone, and iOS. *See Is My Device Supported?*, WHATSAPP, https://www.whatsapp.com/faq/en/general/20951556 (last visited Sept. 13, 2016). iOS is a mobile operating system that has been developed by Apple Inc. *See iOS 10*, APPLE, http://www.apple.com/in/ios/ios-10/ (last visited Sept. 13, 2016). For more information, see *Frequently Asked Questions*, WHATSAPP, http://www.whatsapp.com/faq/en/general (last visited Sept. 13, 2016).

95. *See What Is Voice Messaging?*, WHATSAPP, https://www.whatsapp.com/faq/en/general/25118341 (last visited Sept. 13, 2016). Voice messages refer to messages by which the WhatsApp user can send an audio message to another WhatsApp user or a group of WhatsApp users by using the microphone functionality. *Id.*

96. *See Sending Media and Other Data*, WHATSAPP, https://www.whatsapp.com/faq/en/general/23766198 (last visited Sept. 13, 2016). Media messages are messages through which WhatsApp users can exchange media content, such as photos, with one another. *Id.*

97. Press Release, Office of the Privacy Comm'r of Can., WhatsApp's Violation of Privacy Law Partly Resolved After Investigation by Data Protection Authorities (Jan. 28, 2013), http://www.prnewswire.com/news-releases/whatsapps-violation-of-privacy-law-partly-resolved-after-investigation-by-data-protection-authorities-188654711.html.

reasons, including security.[98] The rest of this Part critically evaluates the decisions of the Dutch DPA on WhatsApp's data retention and encryption practices to highlight their weaknesses in the cloud context.

When considering some of WhatsApp's data retention practices (for example, the retention period of the personal data of inactive users or non-WhatsApp users) the Dutch DPA did not consider how WhatsApp handles the data after the expiry of the retention period.[99] In other words, the Dutch DPA did not examine WhatsApp's data deletion practices.[100]

This is surprising given the close connection between data retention and data deletion in the Data Protection Directive.[101] It would have been important for the Dutch DPA to analyze how data deletion takes place. Does WhatsApp delete only pointers to the data? When are the data permanently (as far as technically possible) deleted? What types of information does WhatsApp store? Does WhatsApp delete all relevant data (including data fragments) at all storage points? Is data deletion permanent or can deleted data be recovered? How do WhatsApp's storage practices differ from platform to platform (for example, iOS)? These are important questions that the Dutch DPA should have considered to understand fully the data deletion and retention practices of WhatsApp.

Initially, the Dutch DPA determined that WhatsApp was in breach of the Dutch data protection laws because WhatsApp transmitted user messages in an unencrypted form.[102] However, at the later stages of the WhatsApp Investigation, the Dutch DPA was satisfied that WhatsApp did not breach the law on this point since by then WhatsApp had implemented end-to-end encryption for its user messages.[103] From the investigation report, it is unclear whether the Dutch DPA fully tested the end-to-end encryption implemented by WhatsApp.[104] Does WhatsApp have an effective key management policy in place? Does the encryption method cover all or specific types of user messages, such as audio and photographs? Is the encryption key secure on all platforms on which WhatsApp can be installed?[105] These are some of the main questions that the Dutch DPA should have pursued. A recent forensic analysis of WhatsApp's installation on the Android platform (the platform tested during the WhatsApp Investigation) has concluded that WhatsApp uses the same Advanced Encryption Standard (AES) with a 192-bit encryption key for all

98. *See* WHATSAPP FINDINGS, *supra* note 92, at 3 ("At the start of the investigation, the Dutch DPA and the OPC identified two security shortcomings . . . . For this reason, WhatsApp was acting in breach of the provisions of article 13 of the Wbp.").

99. *Id.* at 33.

100. *Id.*

101. *Guide to Data Protection: Retaining Personal Data (Principle 5)*, INFO. COMM'R'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/ (last visited Sept. 13, 2016).

102. WHATSAPP FINDINGS, *supra* note 92.

103. *Id.*

104. *Id.* at 6 n.15, 7 n.17.

105. For more on the security issues that can be raised on Android and iOS, see Robert Lemos, *Android vs. iOS Security Comparisons Get Complicated*, EWEEK (July 31, 2014), http://www.eweek.com/security/android-vs.-ios-security-comparisons-get-complicated.html.

end-to-end WhatsApp chat messages.[106] However, until recently, WhatsApp did not encrypt other content, including audio, videos, and photographs.[107]

Having critically analyzed some of the main legal provisions relevant to Cloud Investigations, in the remaining Parts of this Article, I use a decentralized approach to law and Cloud Investigations to shed light on the roles of data protection laws during this regulatory process. Before delving into this matter, though, it is first helpful to understand what this decentralized approach entails.

IV. ORDERING "AT A DISTANCE": CLOUD INVESTIGATIONS AND DATA PROTECTION LAWS

My decentralized view on law and Cloud Investigations is derived from the ideas developed by Michel Foucault and other authors who build on his work.[108] Four interconnected concepts inform my view on Cloud Investigations and law, namely, power, "governmentality," "centers of calculation," and "action at a distance."[109]

In brief, Foucault argues that power does not emanate from only one single source or one single direction (for example, the state or top-down).[110] Rather, power emanates from multiple sources and directions (that is, also bottom-up).[111] Power constitutes "the multiplicity of force relations immanent in the sphere in which [it] operate[s] and which constitute [its] own organization."[112] Despite not emanating from a single source of central authority, power is omnipresent because:

> [I]t is produced from one moment to the next, at every point, or rather in every relation from one point to another. Power is everywhere, not because it embraces everywhere, but because it comes from everywhere.[113]

As such, power can only be exercised. Power is not the appertunance of the privileged few.[114] Rather, power is the "overall effect of [relevant]

106. Neha S. Thakur, Forensic Analysis of WhatsApp on Android Smartphones (Aug. 6, 2013) (unpublished Master's Thesis, Univ. of New Orleans), http://scholarworks.uno.edu/cgi/viewcontent.cgi?article=2736&context=td.

107. *End-to-End Encryption*, WHATSAPP, https://www.whatsapp.com/faq/en/general/28030015 (last visited Sept. 13, 2016).

108. For example, Graham Burchell, Mitchell Dean, Colin Gordon, Bruno Latour, John Law, Thomas Lemke, Peter Miller, Pat O'Malley, Nikolas Rose, and Marianna Valverde, whose works are cited in this Part.

109. *See, e.g.*, Bruce Curtis, *Foucault on Governmentality and Population: The Impossible Discovery*, 27 CAN. J. SOC. 505 (2002) (describing Foucault's concept of governmentality); Heike Jöns, *Centre of Calculation*, *in* THE SAGE HANDBOOK OF GEOGRAPHICAL KNOWLEDGE 158 (2011) (describing "centre[s] of calculation"); ANDREW BARRY ET AL., FOUCAULT AND POLITICAL REASON 43 (1996) (describing "action at a distance").

110. *See* 1 MICHEL FOUCAULT, THE HISTORY OF SEXUALITY: AN INTRODUCTION (1978).

111. *Id.*

112. *Id.* at 92.

113. *Id.* at 93.

114. *Id.*

strategic positions."[115]

"Governmentality" is apposite here as it facilitates our understanding of how the relationships between multiple actors are strategically organized.[116] "Governmentality" refers to the "conduct of conduct"[117] or in "the broad sense . . . [to] techniques and procedures for directing human behavior . . . [g]overnment of children . . . of souls and consciences . . . of a household, of a state, or of oneself" to achieve definite and shifting ends and with often unpredictable outcomes, effects, or consequences.[118] "Governmentality" enables us to analyze the attempts of multiple authorities and agencies to shape the conduct of actors through complex webs of knowledge, techniques, and tactics to achieve "economy" for the population, which becomes crucial in defining the aims of government.[119] Government refers to "an activity that undertakes to conduct individuals throughout their lives by placing them under the authority of a guide responsible for what they do and for what happens to them."[120]

By thinking of a Cloud Investigation in terms of "governmentality," I analyze it as a means of ordering relations between relevant actors in order to achieve specific ends, such as protecting personal data rights.[121] "Governmentality" highlights the mundane, intricate, and diversified practices, routines, skills, and bodies of knowledge that interconnect to render the field of governance amenable to intervention by multiple actors during Cloud Investigations.[122] It also underscores the new forms of inquiry, such as code testing, that shed light on the data protection compliance of the investigated companies in order to achieve particular aims, for example, protecting personal data rights.

The "governmentality" perspective also draws our attention to how "inscriptions," such as the annotations made by the Cloud Providers when filling out the questionnaires of the EU DPAs, enable power to be exercised

115. MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 26–27 (1977).

116. For more on governmentality, see Nikolas Rose et al., *Governmentality*, 2 ANN. REV. L. & SOC. SCI. 83 (2006) and Thomas Lemke, *The Birth of Bio-Politics: Michel Foucault's Lecturer at the College de France on Neo-Liberal Governmentality*, 30 ECON. & SOC'Y 190 (2001).

117. *See* Michel Foucault, *Governmentality*, *in* THE FOUCAULT EFFECT: STUDIES IN GOVERNMENTALITY 87 (Graham Burchell et al. eds., 1991) (describing the concept of governmentality as a phenomenon); MITCHELL DEAN, GOVERNMENTALITY: POWER AND RULE IN MODERN SOCIETY 17–24 (2nd ed. 2010) (expanding on Foucault's definition and arguing that there are three key elements that can be derived from this definition, namely, the degree of calculation as to how conduct is guided, the way in which an individual conducts himself or herself, and the regulation of an individual's behavior in accordance with a specific standard or norm).

118. Michel Foucault, *On the Government of the Living*, *in* 1 ETHICS: SUBJECTIVITY AND TRUTH: ESSENTIAL WORKS OF MICHEL FOUCAULT, 1954–1984, at 81 (Paul Rabinow ed., Robert Hurley trans., 1997); *see also* Colin Gordon, *Governmental Rationality: An Introduction*, *in* THE FOUCAULT EFFECT: STUDIES IN GOVERNMENTALITY 1 (Graham Burchell et al. eds., 1991).

119. Gordon, *supra* note 118, at 1.

120. Michel Foucault, *Security, Territory, Population*, *in* 1 ETHICS: SUBJECTIVITY AND TRUTH: ESSENTIAL WORKS OF MICHEL FOUCAULT, 1954–1984, at 67 (Paul Rabinow ed., Robert Hurley trans., 1997).

121. Michel Foucault, *Governmentality*, *in* THE FOUCAULT EFFECT: STUDIES IN GOVERNMENTALITY 87, 95 (Graham Burchell et al. eds., 1991).

122. *Id.* at 101.

over actors that may be distant from one another.[123] "Inscriptions"—or material and graphical representations of a thing in a durable or mobile form, such as a tabular representation of the storage options of the cloud service—become key here as they provide significant information to actors such as the EU DPA's legal and technical staff so that they can later "act upon" or attempt to order elements that are spatially and organizationally distant from them.[124] Data centers located in various jurisdictions are examples of such elements. Numerous "inscriptions" generated from different locales—such as the "inscriptions" made by the software engineer when designing a specific technology and the "inscriptions" made by the legal advisers when amending or drafting a specific contract, for example a Privacy Notice—are aggregated, compared, compiled, and analyzed by the EU DPA during the Cloud Investigation.[125] These heterogeneous "inscriptions" are brought together in one local "center of calculation," such as the office of the commissioner of an EU DPA, to enable this local center to act upon the entity in question.[126] Power here is very much an "achievement," which depends in part on constantly harnessing multiple sources of information about the data processing practices and operations of the Cloud Provider.[127]

"Governmentality" is particularly useful when studying Cloud Investigations because this perspective enables me to avoid two key problems found in the data protection literature on the powers of EU DPAs. First, the "governmentality" perspective prevents me from limiting my analysis to the actions of the state and its agents only. Second, the "governmentality" perspective enables me to conceive of law in broader terms than the current data protection law literature does. Consequently, I do not approach law only as a binding set of rules that are complied with, breached, or enforced. This vantage point, often used in the data protection literature, focuses only on the determinate side of law in the sense of definite norms to be complied with.[128]

Importantly, the "governmentality" perspective sheds light on law's responsiveness when it is applied in a specific context.[129] Just like other laws, data protection laws do not operate in a vacuum but constantly engage with other sources of power, resistance, and so on when they are applied in practice.[130] Consequently, applying data protection laws is an "import-export

123. *See* Bruno Latour, *Visualisation and Cognition: Drawing Things Together*, *in* REPRESENTATIONS IN SCIENTIFIC PRACTICE 19, 35–44 (Michael E. Lynch & Steve Woolgar eds., 1990); John Law, *On the Methods of Long Distance Control: Vessels, Navigation and the Portuguese Route to India*, *in* POWER, ACTION AND BELIEF: A NEW SOCIOLOGY OF KNOWLEDGE?, 32 SOCIOLOGICAL R. MONOGRAPH 234, 251 (John Law ed., 1986); Peter Miller & Nikolas Rose, *Governing Economic Life*, 19 ECONOMY AND SOCIETY 1, 31 (1990).

124. Latour, *supra* note 123, at 8.

125. *Id.* at 13.

126. *Id.*

127. *Id.*

128. Miller & Rose, *supra* note 123, at 18.

129. INTERACTIVE SOFTWARE FEDERATION OF EUR., ISFE SUBMISSION ON CONSULTATION ON THE LEGAL FRAMEWORK FOR THE FUNDAMENTAL RIGHT TO PROTECTION OF PERSONAL DATA 6 (2009), http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/isfe_en.pdf.

130. *See* BRUNO LATOUR, THE MAKING OF LAW: AN ETHNOGRAPHY OF THE CONSEIL D'ETAT 55 (Marina Brilman & Alain Pottage trans., 2009) ("[L]aw, like nature, abhors a vacuum . . . .").

job" since data protection laws have an impact on the site of its application and vice versa.[131]

Having outlined the main concepts that inform my analysis, next I deal briefly with the methodology that underpins this Article.

V. METHODS

This Article draws on three main qualitative data collection methods, namely, documentary analysis; observation; and interviews of seven DPAs, four multinational Cloud Providers, and the representatives of two European institutions.[132] Qualitative methods enabled me to examine in detail the experiences and practices of the actors participating in Cloud Investigations.

I analyzed several documents, including the current[133] and future[134] European data protection laws; press releases by relevant stakeholders, including the European Commission[135] and the investigated Cloud Providers;[136] correspondence between the EU DPAs and Cloud Providers during Cloud Investigations;[137] and published Cloud Investigation reports.[138] Additionally, I collected data through observation during the Fourth European Data Protection Days (EDPD) Conference in 2014—a key data protection conference attended by relevant stakeholders.[139] Attending the EDPD Conference enabled me to approach potential interview respondents and collect information about current or future Cloud Investigations.

Finally, interviewing enabled me to consolidate my background knowledge about Cloud Investigations and develop a comprehensive understanding of how Cloud Investigations are used in practice to regulate

131. *Id.* at 123.

132. At times, I interviewed more than one person working for the DPAs, especially when addressing large DPAs.

133. *E.g.*, Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, BGBL. I at 66, *amended by* Gesetz [G], Feb. 25, 2015, BGBL. I at 162, art. 1 (Ger.), http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0008; Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 on Data Processing, Data Files and Individual Liberties], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, p. 227, *amended by* Law 2004-801 of Aug. 6, 2004, http://www.legislationline.org/download/action/download/id/1245/file/2c6afeb365cf84afa6d0de952262.pdf; Data Protection Act 1988 (Act No. 25/1988) (Ir.), http://www.irishstatutebook.ie/eli/1988/act/25/enacted/en/html; Data Protection (Amendment) Act 2003 (Act. No. 6/2003) (Ir.), http://www.irishstatutebook.ie/eli/2003/act/6/enacted/en/html; Data Protection Directive, *supra* note 4.

134. GDPR, *supra* note 4.

135. *E.g.*, Press Release, Viviane Reding, Vice-President, Eur. Comm'n, Strong and Independent Data Protection Authorities: The Bedrock of the EU's Data Protection Reform (May 3, 2012), http://europa.eu/rapid/press-release_SPEECH-12-316_en.htm.

136. *E.g.*, Mark Zuckerberg, *Our Commitment to the Facebook Community*, FACEBOOK: NEWSROOM (Nov. 29, 2011), https://newsroom.fb.com/news/2011/11/our-commitment-to-the-facebook-community/.

137. *E.g.*, Letter from Article 29 Data Protection Working Party to Larry Page, Chief Exec. Officer, Google Inc. (Oct. 16, 2012) [hereinafter Article 29 Letter], https://www.dataprotection.ie/documents/press/Letter_from_the_Article_29_Working_Party_to_Google_in_relation_to_its_new_privacy_policy.pdf.

138. *E.g.*, Article 29 Main Findings, *supra* note 91.

139. The conference was held in Berlin on May 12 and 13, 2014. The website for this annual conference can be found at http://www.euroforum.de/edpd.

personal data. I interviewed EU DPAs[140] and Cloud Providers[141] that had direct experience of Cloud Investigations. I also interviewed the European institutions that played key roles in discussing and promulgating the current and future European data protection laws.[142]

I identified over twenty[143] potential respondents from these three categories of actors by considering the following factors:

- The applicable administrative rules;
- The investigative powers of the EU DPAs;
- The EU DPAs' sizes;
- The offerings of the Cloud Providers (for example, single service or technology, suite of services or technologies, target market, etc.); and
- The ease of access to the respondents.

This sampling strategy enabled me to interview respondents whose experiences were directly relevant to my research questions.[144] After obtaining institutional ethical approval, I approached the potential respondents in person, by e-mail, or through social media communications.[145]

---

140. Interview with the Commissioner of one EU DPA (May 30, 2014) [hereinafter Interview 1]; interview with a senior official of another EU DPA (July 25, 2014) [hereinafter Interview 2]; interview with a senior official of another EU DPA (July 1, 2014) [hereinafter Interview 3]; interview with a senior official of another EU DPA (July 8, 2014) [hereinafter Interview 4]; interview with a senior official of another EU DPA (July 11, 2014) [hereinafter Interview 5]; interview with a senior official of another EU DPA (June 6, 2014) [hereinafter Interview 9]; interview with a senior official of another EU DPA (Dec. 5, 2014) [hereinafter Interview 14]; interview with the head of department of the team of a DPA that conducts Cloud Investigations (Dec. 4, 2014) [hereinafter Interview 15] [collectively, hereinafter EU DPA Interviews].

141. Interview with a senior legal counsel of one large multinational Cloud Provider (July 10, 2014) [hereinafter Interview 10]; interview with a senior legal counsel of another large multinational Cloud Provider (July 8, 2014) [hereinafter Interview 11]; interview with a senior legal counsel of another popular multinational Cloud Provider (Sept. 16, 2014) [hereinafter Interview 12]; interview with another large multinational Cloud Provider (Nov. 4, 2014) [hereinafter Interview 13] [collectively, Cloud Provider Interviews].

142. Interview with a senior representative of one European institution (July 11, 2014) [hereinafter Interview 7); interview with a senior representative of another European institution (June 26, 2014) [hereinafter Interview 8] [collectively, hereinafter European Institution Interviews].

143. There are no rules governing the minimum acceptable sampling size for qualitative interviews. *See, e.g.*, Carol A.B. Warren, *Qualitative Interviewing*, *in* HANDBOOK OF INTERVIEW RESEARCH: CONTEXT AND METHOD 83, 99 (Jaber F. Gubrium & James A. Holstein eds., 2002) (suggesting that twenty to thirty interviews support valid conclusions). However, others argue that fewer than sixty interviews cannot be used to generate valid conclusions. *See, e.g.*, Kathleen Gerson & Ruth Horowitz, *Observation and Interviewing: Options and Choices in Qualitative Research*, *in* QUALITATIVE RESEARCH IN ACTION 199, 223 (Tim May ed., 2002). The general rule of thumb is that the adequate number of qualitative interviews for a research project is always context-specific. ROSALIND EDWARDS & JANET HOLLAND, WHAT IS QUALITATIVE INTERVIEWING? 5–7 (2013); Anthony J. Onwuegbuzie & Nancy L. Leech, *Sampling Designs in Qualitative Research: Making the Sampling Process More Public*, 12 QUALITATIVE REP. 238, 240–42 (2007). The sample size should not be too small to prevent data saturation, theoretical saturation, or informational redundancy. ALAN BRYMAN, SOCIAL RESEARCH METHODS 425 (4th ed. 2012). Additionally, the sample size should not be so large that the researcher is unable to understand the object of study in depth. *Id.* In my present research project, ten to twenty interviews would provide a valid sample, as Cloud Investigations in Europe are a recent phenomenon. Thus, I targeted respondents whose activities are directly relevant to my research questions. For more on the virtues of a small sample (under twenty), see Mira Crouch & Heather McKenzie, *The Logic of Small Samples in Interview-Based Qualitative Research*, 45 SOC. SCI. INFO. 483 (2006).

144. For more on purposive sampling and its validity, see BRYMAN, *supra* note 143, at 416–28.

145. *See* Letter from the Research Ethics Comm., Queen Mary Univ. of London, to author (May 21,

Subsequently, I conducted fourteen interviews with DPAs,[146] Cloud Providers,[147] and European institutions[148] over several days from May 2014 to December 2014. I ensured that my interview sample was valid by, for example, relying on multiple data sources to support a conclusion. All of my interviews were conducted on a non-attributable basis over the telephone or by Skype, depending on the respondent's availability. Consequently, I am unable to provide any information that identifies my respondents, including a list of the interviewed organizations. Most interviews lasted one hour, were audiotaped when the respondent consented, and were fully transcribed. When transcribing the interviews, I ensured that the transcriptions were as close to the interviews as possible by, for example, minimally tidying up the text. I explored various themes during the interviews, including the relationships between the actors during Cloud Investigations and the factors that affect Cloud Investigations (for example, the attitudes of Cloud Providers). I adopted flexible and non-leading interviewing techniques to ensure that the respondents could tell their own stories of Cloud Investigations. I used multiple strategies to manage difficult interviews. For example, when I had to ask commercially or legally sensitive questions, such as when I queried the links between the Snowden revelations and Cloud Investigations, I phrased these questions carefully so that the respondents did not clam up.[149]

I used the following techniques to ensure that my data analysis was rigorous:

- Explanation building;
- Generating explanatory descriptive themes and sub-themes;
- Evaluating how the themes and sub-themes relate to one another;
- Using theoretical notions (such as "action at distance") to generate more abstract themes; and
- Searching for empirical data that challenged my theoretical and empirical assumptions to ensure that my data analysis was valid.

Having explained my methodology, in the next Part, I examine some of my empirical findings on how data protection laws are used during Cloud Investigations.

2014) (granting ethical approval) (on file with author).

146. Cloud Provider Interviews, s*upra* note 141.

147. EU DPA Interviews, s*upra* note 140.

148. European Institution Interviews, *supra* note 142.

149. Edward Snowden is a former contractor of the U.S. National Security Agency (NSA). *Edward Snowden: Leaks that Exposed US Spy Programme*, BBC NEWS (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964. In June 2013, Mr. Snowden leaked the details of extensive Internet and phone surveillance by the NSA. *Id.* These leaks were followed by further revelations in several newspapers that the NSA directly tapped into the servers of various Internet companies, including multinational Cloud Providers, such as Facebook, Google, Microsoft, and Yahoo!, to track online communications. *Id.*

VI. STRATEGIC USE OF DATA PROTECTION LAWS: BARGAINING ENFORCEMENT

In this Part, I analyze how data protection laws can often be strategically deployed during Cloud Investigations by the regulator and regulatee to advance or stall negotiations. Even in cases where the strategic use of laws achieves the aims of the legislators, for example, compliance with the Data Protection Directive (as nationally implemented), such laws are often not deployed in the manner intended by the lawmakers.

To achieve the aims of this Article, selectivity is key, if not essential. There are no doubt cases in which data protection laws are used by EU DPAs during Cloud Investigations in the ways envisaged by lawmakers, for example, to sanction a data breach. However, during my interviews, the respondents have elaborated mostly on the situations where data protection laws have been used in ways not envisaged by the lawmakers. Consequently, I focus in detail on such strategic uses of data protection laws during Cloud Investigations. Notwithstanding, this does not mean that data protection laws are not used in the ways intended by the legislative draftsperson during Cloud Investigations.

My data analysis suggests that both EU DPAs and Cloud Providers can often use data protection laws as bargaining chips during Cloud Investigations. This practice may have evolved out of the broad and discretionary powers of EU DPAs, which means that they can deploy many techniques, including negotiations, to achieve legal and regulatory compliance. Likewise, the time frame of Cloud Investigations—typically one to two years[150]—means that both parties develop a longstanding relationship that can often be distinct from other regulatory relationships, such as the relationship between the Cloud Provider and the judge in a lawsuit, where enforcement is often a once-and-only type decision.

My data analysis highlights four possible bargaining scenarios. In the first scenario, the EU DPA uses threats of fines, lawsuits, or similar enforcement actions under data protection laws to persuade the Cloud Provider to agree to its recommendations during Cloud Investigations.[151] This is the classic example of law's coercive power being invoked to bring about a change in the behavior of the regulatee. Depending on how the Cloud Provider responds, such threats can eventually turn into action as the "last resort" to generate the company's legal compliance.[152]

In the second scenario, the EU DPA seeks to persuade the Cloud Provider to change its processing operations and policies by suggesting that doing so would persuade the EU DPA to refrain from exercising its full legal powers concerning a detected data breach.[153] Several factors, such as the severity of the data breach and how the Cloud Provider responds to the regulator, may

150. *See* EU DPA Interviews, *supra* note 140; Cloud Provider Interviews, *supra* note 141.
151. *See, e.g.*, Interviews 2 & 3, *supra* note 140.
152. Cloud Provider Interviews, *supra* note 141.
153. *See, e.g.*, Interview 1, *supra* note 140.

lead to this bargaining scenario. For example, if the EU DPA concludes that the Cloud Provider has not provided its users with clear and transparent information to explain why certain categories of "personal data" are being processed by the organization in its policies, the EU DPA may seek to cajole the Cloud Provider to amend the wording of its policies. It would do this by promising that it will not sanction the organization for this breach if the company makes the amendment within a given time frame, the alternative being for the EU DPA to impose a sanction straightaway. However, in reality this promise may not be worth as much as it might appear to, because many EU DPAs often attempt to investigate and resolve some of the data protection complaints filed by individuals during their Cloud Investigations.[154] In such cases, if the complainant is not satisfied with the outcomes of the Cloud Investigations (as they relate to his or her complaint), the EU DPA often has to formally investigate the complaint after the Cloud Investigation by using a separate procedure.[155] In effect, this means that although the Cloud Provider may have been persuaded to implement specific operational or policy changes during the Cloud Investigation on the basis that the EU DPA would not exercise its full legal powers, the provider can at times find itself in a situation in which this changes later. It is not clear to what extent both parties articulate this contingency during their negotiations.[156]

In the third scenario, the EU DPA seeks to persuade the Cloud Provider to comply with measures that are not within the ambit of national data protection laws by offering extended benefits. Examples of extended benefits include an EU DPA publicly acknowledging that the Cloud Provider has fully cooperated with the regulator during the Cloud Investigation or an EU DPA positively phrasing the Cloud Provider's compliance with the law in public documents, such as the reports published at the end of the investigation.[157] Some EU DPAs may even publish reports that have been partly drafted by the investigated organization.[158] As one of the EU DPA respondents says: "If you [the Cloud Provider] want us [the EU DPA] to phrase it [your compliance] that way rather than another one, why should we care? . . . If we get the substance of what we want we don't care . . . how it is presented."[159]

In the final scenario, the Cloud Provider can often use legislative provisions to stall negotiations. For instance, in some Cloud Investigations, Cloud Providers argue that they do not fall within the "establishment" provision of the Data Protection Directive (as nationally implemented) and that the EU DPA has no jurisdiction over its activities.[160] Such companies can

154. EU DPA Interviews, *supra* note 140.

155. *See, e.g.*, Data Protection Act 1988 (Act No. 25/1988) (Ir.), *amended by* Data Protection (Amendment) Act 2003 (Act. No. 6/2003) (Ir.), http://www.dataprotection.ie/viewdoc.asp?DocID=796 (informal consolidation) (stating that the Irish Data Protection Authority has to initiate a separate procedure to investigate the complaint of an individual).

156. *See, e.g.*, Interview 1, *supra* note 140.

157. *See, e.g.*, *id.*

158. *Id.*

159. *Id.*

160. Interview 3, *supra* note 140.

often capitalize on some of the uncertainties that arise in the transnational context, in which it may not always be clear where the Cloud Provider is in fact "established" for the purposes of the Data Protection Directive. Under Article 4(1) of the Data Protection Directive, each EEA country has an obligation to apply the Data Protection Directive (as implemented nationally) if:

> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
> (c) the controller is not established on Community territory and for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[161]

As with other aspects of the Data Protection Directive, Article 4 suffers from several weaknesses. Article 4 is vague as it contains a number of unclear phrases, such as "in the context of the activities of an establishment of the controller."[162] Article 4 has also been inconsistently implemented in the EEA.[163] In the cloud context, the concept of "establishment" can often be very problematic as it can often be difficult to determine where a "data controller" is "established" due to the complex cloud chain.[164] Occasionally, a Cloud Provider can question the legitimacy of the Cloud Investigation by arguing that the EU DPA does not have authority to regulate its activities because the company is not "established" in its jurisdiction within the meaning of the Data Protection Directive (as nationally implemented).[165] Legitimacy means that the EU DPA "is perceived as having a right to govern both by those it seeks to govern and those on behalf of whom it purports to govern."[166] The legitimacy argument also raises accountability questions, such as on whose behalf the EU DPAs are acting and whether the EU DPA has the right to call them to account. Here, the Cloud Providers use such arguments to either stall the negotiations or attempt to gain the upper hand during the negotiations.[167]

---

161. Data Protection Directive, *supra* note 4, art. 4(1).
162. *Id.*
163. *See* W. Kuan Hon et al., *Which Law(s) Apply to Personal Data in Clouds?*, *in* CLOUD COMPUTING LAW 246 (Christopher Millard ed., 2013) (describing the uncertainty of law applicability to issues of cloud computing).
164. Hon et al., *supra* note 163, at 246–47.
165. *Id.* at 222–24.
166. Julia Black, *Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes*, 2 REG. & GOVERNANCE 137, 144 (2008).
167. All Interviews, *supra* notes 140–42.

Having analyzed how EU DPAs and Cloud Providers can often use data protection laws as bargaining chips during Cloud Investigations, next I analyze the roles of data protection laws in generating "centers of calculations" during Cloud Investigations. "Centers of calculations" are crucial zones of analysis because decisions about legal compliance are made in these spaces.[168]

VII. MULTIPLE CENTERS OF REGULATION

In this Part, I evaluate how multiple calculations rather than only legal ones come together to generate regulatory effects, such as bringing the Cloud Providers' processing operations in line with the relevant laws. This analysis supports my contention that law can play variable roles during Cloud Investigations, depending on several factors, including the processing operations of the Cloud Providers, the aims and foci of the Cloud Investigations, the socio-political context, and so on. Sometimes law can be at the forefront of activity during Cloud Investigations while at other times law can retreat slightly from sight in the field of action as other actors carry out the act of "government." What are the centers of calculations commonly involved during Cloud Investigations? How do such centers of calculation enable "action at a distance" in the sense of enabling the EU DPA? I address these questions in this Part by examining some of the main calculations that can often be involved during some of the stages of Cloud Investigations.

A. The Three Stages of Cloud Investigations

Before delving into this matter, it would be useful if I explained my empirical findings on the three main stages of Cloud Investigations, namely, the pre-investigative, investigative, and post-investigative stages.[169] Generally speaking, the particular details of these three stages may vary depending on the aims and foci of the investigations, the applicable procedural laws, the national data protection laws, and so on.

Typically, the pre-investigative stage covers all the actions of the relevant parties that lead to the investigative stage. Depending on context, a number of matters can take place during the pre-investigative stage. For example, some EU DPAs can start to engage with the Cloud Provider through e-mail exchanges and conference calls to inform the company that the regulator may wish to formally investigate the organization in the forthcoming months.[170] Other EU DPAs provide the Cloud Providers with detailed information about the subsequent investigative process and how they can get ready for the forthcoming investigation.[171] Other EU DPAs can spend quite a lot of time during this stage to understand the business model, processing operations, and

168. Jöns, *supra* note 109, at 158–70.
169. *E.g.*, All Interviews, *supra* notes 140–42.
170. *Id.*
171. *Id.*

corporate structure of the company.[172]

The investigative stage starts when the EU DPA formally initiates the Cloud Investigation by, for example, sending a letter of intention to investigate to the Cloud Provider, and ends when the report is finalized and/or published (not all reports are published). This stage has three main aspects, which can be iterative, namely, fact-finding, negotiations, and decision-making. Typically at the start of the investigative stage, the EU DPA gathers evidence about the Cloud Provider's compliance with data protection laws. The types of evidence collected vary depending on the context in question but can include internal and external data protection documents, algorithmic sequences performing a specific operation, such as data deletion, and so on.

Based on its review of such evidence and its discussion with the Cloud Provider, the EU DPA then decides about the provider's compliance in its processing operations and policies with the relevant laws.[173] Cloud Providers play an active role during the investigative stage by, for example, providing the EU DPAs with the relevant evidence, challenging how EU DPAs understand their operations, and clarifying their policies.[174] Toward the end of the investigative stage, many EU DPAs usually reach preliminary decisions about the data protection compliance of the organization.[175] Such decisions are either finalized or amended following negotiations with the Cloud Provider.[176] Typically, when negotiations take place during a Cloud Investigation, they can be quite lengthy, as both parties seek to reach mutually acceptable solutions. These are data protection solutions that bring the Cloud Provider's operations and policies in line with the relevant laws and do not damage the business interests of the company. Once the EU DPA has reached a final decision about the Cloud Provider's data protection compliance, the regulator details the findings of the Cloud Investigation in a lengthy report, with its recommendations and the timetable for the implementation of the recommendations.[177] Depending on the circumstances in question, the report can be either privately or publicly disseminated.[178]

Finally, the post-investigative stage refers to the period following the dissemination (whether internal or external) of the investigation report.[179] Typically at this point, the EU DPA monitors whether the Cloud Provider is implementing its recommendations within the set time frame.[180] The Cloud Provider can also ask the EU DPA for further practical advice on how to implement certain recommendations or advice on future changes to its

172. *Id.*
173. *Id.*
174. *Id.*
175. *Id.*
176. *Id.*
177. *Id.*
178. *Id.*
179. *Id.*
180. *Id.*

processing operations or policies.[181]

So what accounts of compliance are produced during these different stages of Cloud Investigations? By whom? I answer these questions next by focusing on some of the typical accounts of compliance that are produced during the pre-investigative and investigative stages of Cloud Investigations. I do not analyze the accounts of compliance involved post-investigation, because many Cloud Investigations are in the early stages of post-investigation. Consequently, I do not have enough data to evaluate comprehensively the "centers of calculation" involved during this phase.

B. Generating Compliance Accounts During Cloud Investigations

During the pre-investigative phase, multiple accounts of compliance can be generated by different actors depending on the investigation in question. For instance, an EU DPA that is unfamiliar with the data processing operations and business model of a Cloud Provider may engage in substantial discussions with various teams of the Cloud Provider, such as management, engineering, and legal, to know more about the entity it will regulate later.[182] Such discussions often generate several accounts of compliance; which involve various types of information, data protection policies, staff guidance on all aspects of data protection, and privacy permission screens.[183] Such discussions often generate several accounts of compliance, which involve various types of information, data protection policies, staff guidance on all aspects of data protection, and privacy permission screens.[184] Other "centers of calculations" can also be involved, including identifying the accounts of compliance that the company will need to provide to the regulator during the subsequent investigative stage, establishing the types of evidence that support these compliance accounts (such as data logs), and pinpointing the locations of such evidence.[185] This can often be tricky in cloud ecosystems.[186] Formal data protection laws can often underpin various calculations, such as evaluating the data protection compliance accounts that the organization needs to provide to the regulator by referring to the relevant legislative framework. However, and crucially for our purposes, the production of such accounts, which can often be vital to the regulator during the subsequent investigative stage, depends on other actors, who may or may not bring particular legal considerations with them when carrying out such tasks.

During the investigative stage, other accounts of compliance are generated, often by similar and at times new actors. For instance, depending

181. *Id.*

182. Interview 1, *supra* note 140.

183. *See, e.g.*, Daniel P. Cooper, *Corporate Investigations & EU Data Privacy Laws—What Every In-House Counsel Should Know*, COVINGTON & BURLING LLP (2008), https://www.cov.com/~/media/files/corporate/publications/2008/01/corporate-investigations-and-eu-data-privacy-laws-amended-20-9-08.pdf (describing the kinds of issues that arise during the pre-investigative phase).

184. EU DPA Interviews, *supra* note 140.

185. *Id.*

186. Interview 12, *supra* note 141.

on the aims and foci of the Cloud Investigation, the EU DPA may seek accounts of how specific technical functions, such as the encryption of messages, are performed to evaluate whether the Cloud Provider complies with its security and confidentiality obligations under the relevant national laws.[187] Here, multiple centers of calculation produce different accounts of how this specific security measure operates in practice. As an example, the legal team of the Cloud Provider generates an account of the organization's encryption policies as set out in its internal and external documents. The technical team of the Cloud Provider produces a different account of how encryption operates at a technical level. Such technical accounts may focus on key issues, including the encryption method, encryption key length, key access, the points at which data are encrypted, and whether the whole or part of the dataset is encrypted. Although data protection laws can often constitute some of the accounts, as with the pre-investigative phase, the production of these accounts does not depend solely on legal actors or factors.

Durable and mobile "inscriptions" become key here in enabling "action at a distance" because such inscriptions are later "acted upon" by other actors. For instance, if the data retention or deletion practices of the Cloud Provider are under scrutiny by the EU DPA, the technical team of the Cloud Provider often has to provide the regulator with detailed information of its storage options.[188] Typically, such information can be provided by a table or similar diagram that particularizes the stored data types, their formats, and their locations (for example, /data/data subdirectory or /mnt/sdcard).[189] This table is mobile since it can easily traverse different spaces, like the technical and legal team of the Cloud Provider, the sub-contractor of the EU DPAs, and so on, through instantaneous means, such as electronic mail, without being altered. These "inscriptions" play an important part in regulating "personal data" because they provide to the regulator reliable information on specific processing operations, such as the Cloud Provider's storage practices. If this information was not reliably transmitted to the regulator, the latter would be unable to assess whether, and to what extent, the Cloud Provider's storage policies comply with the relevant laws. These diverse compliance accounts are then reviewed or tested by many actors on the EU DPA end to evaluate to what extent the Cloud Provider adheres to data protection laws.[190]

Many EU DPAs can also collect other forms of evidence during the investigative stages by using various actors. The precise actors involved depend on a number of considerations, including how the EU DPA organizes its operations and the EU DPA's resources. Some EU DPAs with a limited number of staff may employ sub-contractors to test whether all the relevant algorithmic codes operate in the manner set out in the data or security policies

187. EU DPA Interviews, *supra* note 140.
188. *Id.*
189. *Id.*
190. *Id.*

of the Cloud Provider.[191] The sub-contractors provide a detailed account of each operation that has been technically tested, in a durable and mobile medium, such as a report, which is then later "acted upon" by the EU DPA.[192] Other EU DPAs may ask specialist state agencies, such as the Financial Police, to inspect the premises and servers of the Cloud Provider.[193] Despite the divergence in terms of the actors involved during the fact-finding phase of an investigation, typically these actors review particular aspects of compliance, such as how the Cloud Provider handles personal information on a technical level, rather than conduct an overarching review of compliance, which happens later in the investigation.

As I mentioned earlier, although data protection laws underpin several aspects of these evaluations, such as determining which technical operations should be examined, the focus here can often be very much on examining key matters, for example, how cookie installation and deletion work in practice. Particular modes of inquiries, for instance real-time evaluation of how the staff of the Cloud Providers deals with security and data protection concerns, can often be used here to determine data protection compliance rather than merely reviewing a privacy policy. EU DPAs that use such types of inquiries tend to have either a higher or equal number of technically trained staff, as opposed to legally trained staff, to determine if the Cloud Provider is "*accountable in reality*" (my emphasis).[194] Having said that, the precise mix of legal and technical staff deployed in a Cloud Investigation depends on several factors, including the EU DPA's resources, the technical complexity of the investigation, and the stage of the investigation. Some EU DPAs use an equal mix of legal and technical staff.[195] Other EU DPAs may deploy more technical rather than legal staff during their Cloud Investigations.[196] For others still, the legal staff can often take a backseat role during the fact-finding phase of the investigations as the technical staff carries out most of the evaluation. Here, the legal staff tends to take on a more significant role during the decision-making and negotiation stages.[197] Consequently, for such EU DPAs during the early phases of Cloud Investigations, formal data protection laws may not always be visible in the field of action although they operate in the background.

For many EU DPAs, even when they have reached the later stages of the investigation and are forming overarching decisions about the Cloud Provider's legal compliance, they focus on whether the company is accountable in reality rather than whether the organization has only implemented data protection laws in its "fancy privacy policy."[198] As one of

191. *Id.*
192. *Id.*
193. *Id.*
194. Interview 1, *supra* note 140.
195. *See, e.g.*, Interview 2, *supra* note 140.
196. *See, e.g.*, Interview 1, *supra* note 140.
197. *See, e.g.*, Interview 14, *supra* note 140.
198. Interview 1, *supra* note 140.

the EU DPA respondents says:

> We tend to be substance-oriented people . . . . We want to find out in reality are you implementing the law? So we certainly will read your privacy policy but that is not necessarily our focus . . . . We often hear the criticism that some EU DPAs are just focused on legal. We are not. We are focused on substance. So our approach is show me . . . . Show me what you are doing with the data. What's the security? Does this person have access to this data? Why? What do you mean you are providing access to this data to those people? So we will certainly be checking the legal basis but it's the legal basis for the substance. We will not spend hours agonizing over the finer points of your privacy policy. Your privacy policy is only your starting point. We are focusing on: is this company in reality accountable? Not, does it have a fancy privacy policy?[199]

The above extract is very significant as it illustrates that many EU DPAs focus on whether (and to what extent) the Cloud Provider can demonstrate legal compliance in reality.

These multiple accounts are examined by the EU DPA toward the end of the Cloud Investigation to determine the compliance of the Cloud Provider with the relevant data protection laws.[200] Here, there is evidently a very close link between the accounts produced during the Cloud Investigation and the outcomes of the Cloud Investigations. Outcomes include the compliance recommendations of the EU DPAs. This does not mean that accounts of compliance cannot be constructed in specific ways so that a particular version of compliance is generated, especially when the report produced at the end of the Cloud Investigation is published.

From the above, we can understand that data protection laws do not have privileged or static roles during Cloud Investigations. At times, law can be at the forefront of the activity during the Cloud Investigations, for instance, to determine the applicable norm. At other times, law works in conjunction with other elements, such as technological and social ones, to generate compliance accounts and, ultimately, regulation. For example, an inquiry into the data minimization procedures of the Cloud Provider is an account that focuses on legal, technological, and social matters such as the management's involvement in designing technologies or policies that protect personal data, the data minimization rule, and the technical personal data processing operations.

VIII. CONCLUSION

In this Article, I have advanced two main arguments. First, during Cloud Investigations, EU DPAs and the Cloud Providers can use the legal framework to achieve multiple ends, some of which are not (explicitly at least) embodied

199. *Id.*
200. EU DPA Interviews, *supra* note 140.

in the law itself. Second, I have argued that it should not be assumed that data protection laws dominate the investigative process at all times. Rather, such conclusions should be based on empirical evidence because at times law can disappear from view as other local actors participate in the regulatory process. In many Cloud Investigations the focus is not always on law as it appears in the relevant statute but rather on whether and to what extent the Cloud Provider is "accountable in reality."[201] Determining real accountability means relying on complex modes of inquiries, such as technical testing and real-time evaluation of the alignment between the Cloud Provider's processing operations and policies, which can shed light on how the organization operates in practice rather than in theory.

Going forward, three points should be borne in mind. Although it may be acceptable (although not desirable) for EU DPAs to rely on the truthfulness of the accounts provided by the Cloud Providers during an investigation, without requiring detailed supporting evidence, this practice is likely to become less acceptable when the General Data Protection Regulation (GDPR) applies in May 2018. In particular, the GDPR's explicit recognition of accountability,[202] enhanced rights for "data subjects,"[203] and stricter obligations for both "controllers" and "processors"[204] mean that Cloud Providers will inevitably have to provide their regulators with more detailed and reliable evidence of their legal compliance. As an example, nowadays, even in cases where the EU DPA reviews portions of the algorithms to determine whether the processing operations of the Cloud Provider complies with the law, the EU DPA has to trust that the company has provided the regulator with the algorithmic sequence that is actually implemented. Consequently, one of the tasks ahead is to evaluate how EU DPAs can obtain suitable and adequate accounts of compliance during investigations.

Related, a second task ahead is for EU DPAs to provide guidance to investigated companies on the appropriate measures, tools, and practices that they should adopt in order to comply with and demonstrate their compliance with data protection laws to relevant stakeholders, such as the EU DPAs and the data subjects. DPAs should act in concert with one another when producing such guidance in order to promote a transnational approach to compliance as well as reduce legal uncertainty, legal inconsistency, and compliance costs. Finally, if Cloud Investigations are to achieve their regulatory aims, it is important that EU DPAs investigate cloud-centric issues during their Cloud Investigations rather than only general data protection issues. Currently, data protection issues specific to the cloud, such as data deletion in highly fragmented ecosystems, are not adequately scrutinized during Cloud Investigations.

In all likelihood, as cloud computing is adopted more widely in Europe, it

201. Interview 1, *supra* note 140.
202. *E.g.*, GDPR, *supra* note 4, art. 5(2).
203. *Id.* ch. III.
204. *Id.* arts. 24–28, 30, 32–37.

is inevitable that more cloud-based companies will come under the scrutiny of European regulators. By ignoring cloud-centric issues during Cloud Investigations, EU DPAs are at severe risk of ignoring key data protection concerns raised by particular cloud ecosystems and obtaining only partial views of compliance during the investigative process. This also has serious implications for the trust of the public in the efficacy of the investigative process in obtaining a full account of the compliance of the Cloud Provider with the relevant data protection laws.